

AMC
MK

Steven T. Wax, OSB #85012
Federal Public Defender
101 SW Main Street, Suite 1700
Portland, Oregon 97204
Tel: 503-326-2123
Fax: 503-326-5524
steve_wax@fd.org

Amicus Curiae

UNDER
SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON

IN THE MATTER OF THE
APPLICATION OF THE UNITED
STATES OF AMERICA FOR A
SEARCH WARRANT FOR
CONTENTS OF ELECTRONIC
MAIL AND FOR AN ORDER
DIRECTING A PROVIDER OF
ELECTRONIC COMMUNICATION
SERVICE TO NOT DISCLOSE THE
EXISTENCE OF THE SEARCH
WARRANT,

No. 08-mc-9147

BRIEF OF
AMICUS CURIAE

TABLE OF CONTENTS

	PAGE
I. The Stored Communications Act (SCA) At Issue In This Case Was Enacted To Provide Privacy Protections To Electronic Communications	2
II. The Government's Challenge To The Magistrate Judge's Order Is Based On A Mischaracterization Of The Statute By Injecting a Word – Obtains– That Is Not Part Of The Statutory Text	3
A. The Plain Meaning Of Section 2703(a) Incorporates All Rule 41 Provisions, Including The Notice Requirements	4
B. The Canons Of Statutory Construction Support The Plain Meaning Requiring Notice To The Subscriber or Customer Of The Execution Of A Warrant	6
III. The Amendments Promulgated Pursuant To The Patriot Act Did Not Change The Plain and Unambiguous Meaning Of the Statute	13
IV. If There Were Any Ambiguity, The Doctrine Of Constitutional Avoidance Requires Notice	15
A. A Search Pursuant To A Warrant Without Any Notice To The Subscriber Violates The Fourth Amendment	16
Conclusion	21

TABLE OF AUTHORITIES

	PAGE
<i>Barnhart v. Peabody Coal Co.</i> , 537 U.S. 149 (2003)	7
<i>Berger v. New York</i> , 388 U.S. 41 (1967)	20
<i>Boumediene v. Bush</i> , 128 S. Ct. 2229 (2008)	15
<i>California v. Acevedo</i> , 500 U.S. 565 (1991)	11
<i>Clark v. Martinez</i> , 543 U.S. 371 (2005)	15
<i>Crooks v. Harrelson</i> , 282 U.S. 55 (1930)	4
<i>Dalia v. United States</i> , 441 U.S. 238 (1979)	19, 20, 21
<i>Dolan v. Postal Service</i> , 546 U.S. 481 (2006)	9, 10
<i>Duncan v. Walker</i> , 533 U.S. 167 (2001)	8
<i>Erlerbaugh v. United States</i> , 409 U.S. 239 (1972)	10
<i>Ex parte Jackson</i> , 96 U.S. 727 (1878)	18
<i>Garcia v. United States</i> , 469 U.S. 70 (1984)	4
<i>Gerstein v. Pugh</i> , 420 U.S. 103 (1975)	21

<i>Griffin v. Oceanic Contractors, Inc.</i> , 458 U.S. 564 (1982)	10
<i>In Re Search Of Yahoo, Inc.</i> , No. 07-3194-MB, 2007 WL 1539971 (D.Ar z. 2007)	14
<i>In re Search Warrant</i> , No. 6:05-MC-168-orl-31J66, 2005 WL 3844032 (M.D.Fla. 2005)	14
<i>In the Matter of Seizure of Property Belonging to Talk of the Town Bookstore, Inc.</i> , 644 F.2d 1317 (9th Cir.1981)	11
<i>Jimenez v. Quarterman</i> , 129 S. Ct. 681 (2009)	4
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	16, 17, 21
<i>Lamie v. United States Trustee</i> , 540 U.S. 526 (2004)	4
<i>Montclair v. Ramsdell</i> , 107 U.S. 147 (1883)	8
<i>Quor v. Arch Wireless Operating Company, Inc.</i> , 529 F.3d 892 (9th Cir. 2008)	18
<i>Russello v. United States</i> , 464 U.S. 16 (1983)	6
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	17, 19
<i>TRW Inc. v. Andrews</i> , 534 U.S. 19 (2001)	8
<i>Tennessee Valley Authority v. Hill</i> , 437 U.S. 153 (1978)	4
<i>United States v. Barth</i> , 26 F. Supp. 2d 929 (W.D. Tex. 1998)	18
<i>United States v. Berkos</i> , 543 F.3d 392 (7th Cir. 2008)	14

<i>United States v. Chadwick</i> , 433 U.S. 1 (1977)	11
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008)	18
<i>United States v. Freitas (Freitas II)</i> , 856 F.2d 1425 (9th Cir. 1988)	21
<i>United States v. Freitas (Freitas I)</i> , 800 F.2d 1451 (9th Cir. 1986)	19, 20, 21
<i>United States v. Gantt</i> , 194 F.3d 986 (9th Cir. 1991)	3, 21
<i>United States v. Heckenkamp</i> , 482 F.3d 1142 (9th Cir. 2007)	18
<i>United States v. Menasche</i> , 348 U.S. 528 (1955)	8
<i>United States v. New York Telephone Co.</i> , 434 U.S. 159 (1977)	17
<i>United State v. Ron Pair Enterprises</i> , 489 U.S. 235 (1989)	6
<i>United States v. Villegas</i> , 899 F.2d 1324 (2d Cir. 1990)	19
<i>United States v. W.R. Grace</i> , 526 F.3d 499 (9th Cir. 2008)	3
<i>United States v. Williams</i> , 128 S. Ct. 1830 (2008)	11
<i>Warshak v. United States</i> , 490 F.3d 455 (6th Cir. 2007)	17, 18, 19

FEDERAL STATUTES AND RULES

18 U.S.C. § 2701	1
------------------------	---

18 U.S.C. § 2702	10
18 U.S.C. § 2703	2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 22, passim
18 U.S.C. § 2704(a)(2)	9
18 U.S.C. § 2705	3, 7, 9, 13, 16
1983 U.S.C.C.A.N.	14, 15
Fed R. Crim. P. 41	3, 4, 5, 6, 7, 8, 10, 11, 13, 16, 19, 20, 22, 23

The Federal Defender for the District of Oregon has been assigned by this Court to file an amicus curiae brief opposing the government's appeal of Magistrate Judge Hubel's order that the government provide notice to the subscribers of e-mail accounts whose records have been seized from third-party service providers pursuant to a federal search warrant.¹ The Magistrate Judge did not require immediate notice, but rather, ordered that, after a prolonged period of investigation, the government was required to provide notice to persons whose electronic information had been seized. Amicus curiae believes that the statutes and Constitution do not permit the government to hide forever from the subjects of a search that their privacy has been intruded upon. This pleading argues that the rules of statutory construction support the order under review, that the legislative history supports the protection of privacy that the order provides, and that the doctrine of constitutional avoidance counsels against an interpretation of the statute that would deprive the aggrieved persons whose records have been seized from ever learning that their privacy has been invaded.

I. The Stored Communications Act (SCA) At Issue In This Case Was Enacted To Provide Privacy Protections To Electronic Communications.

18 U.S.C. § 2701 *et seq.* was enacted to provide privacy protections to electronic communications in the control of communications providers. It was passed in 1986, a time when e-mail communications were first beginning to become commonplace and Congress realized that there was a potential gap in the legal protections afforded such

¹The Federal Public Defender's Office is also appointed amicus curiae in Case No. CR 08-mc-9131-A. While the government has only appealed Case Nos. CR 08-mc-9147 A and B, counsel for the government believes the resolution of the appeal in this case will also affect Magistrate Judge Hubel's Order in CR 08-mc-9131-A.

communications. The chapter generally prohibits third party access to electronic communications. 18 U.S.C. § 2703 is a limitation on the protections and authorizes governmental seizures based on traditional constitutional concepts of probable cause and reasonable suspicion. The statute references the Federal Rules of Criminal Procedure.

Recognizing that communications may be worthy of greater or lesser protection based on their age or the type of storage facility in which they are kept, Congress provided different degrees of protection in each subsection of § 2703. Of particular relevance to this appeal, Congress differentiated between the requirements of notice in each subsection, including a provision in subsection (b) that dispenses with notice but not including any such provision in subsection (a). Specifically at issue in this case are 18 U.S.C. § 2703 (a) and (b). Subsections (a) and (b) of § 2703 provide in relevant part:

(a) Contents of wire or electronic communications in electronic storage. – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service. – (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) without required notice to the subscriber or customer, if the

governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity –

- (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
- (ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to Section 2705 of this title.

The government's view of the statute undermines one of the central functions of Rule 41 – providing judicial oversight throughout the warrant process to protect against unnecessary government intrusions and to ensure that citizens have the opportunity to object to improper intrusions. *See United States v. Gantt*, 194 F.3d 986, 1001 (9th Cir. 1991), overruled on other grounds, *United States v. W.R. Grace*, 526 F.3d 499 (9th Cir. 2008). Warrant execution and return procedures are the means by which a warrant is subject to judicial oversight. Accordingly, the government's position that the warrant execution and return procedures do not apply to warrants for stored electronic communications cannot be reconciled with the purpose of Rule 41 and is inconsistent with the government's later concession that a § 2703(a) warrant must be "supported by probable cause and *subject to judicial review*." Br. at 10 (emphasis added).

II. The Government's Challenge To The Magistrate Judge's Order Is Based On A Mischaracterization Of The Statute By Injecting a Word – Obtains– That Is Not Part Of The Statutory Text.

The government reads 18 U.S.C. § 2703(a) as incorporating only those procedures in Fed. R. Crim. P. 41 for obtaining and issuing a warrant, not those relating to the warrant's execution. In its brief, the government claims, "Section 2703(a) allows the government to *obtain* e-mail content in electronic storage for 180 days or less only if

it *obtains* a ‘warrant issued using the procedures described in the Federal Rules of Criminal Procedure.’ Br. at 6 (emphasis added). This is so, the government argues, because “the cross-reference to Rule 41 only refers to the specific procedural provisions of *obtaining and issuing* search warrants.” Br. at 6 (emphasis in original). In seeking to limit the incorporation of only those provisions of Rule 41 that relate to obtaining warrants, the government fundamentally alters the statute’s plain meaning.

A. The Plain Meaning Of Section 2703(a) Incorporates All Rule 41 Provisions, Including The Notice Requirements.

In all statutory construction cases, the first step is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case. *Jimenez v. Quarterman* 129 S.Ct. 681, 685 (2009) (citing *Lamie v. United States Trustee*, 540 U.S. 526, 534 (2004)). Where no ambiguity appears in the statute, “judicial inquiry is complete, except in ‘rare and exceptional circumstances.’” *Garcia v. United States*, 469 U.S. 70, 75 (1984) (quoting *Tennessee Valley Authority v. Hill*, 437 U.S. 153, 187 n.33 (1978) (quoting *Crooks v. Harrelson*, 282 U.S. 55, 60 (1930))). In this case, the plain language unambiguously incorporates all of the warrant requirements in the Federal Rules of Criminal Procedure, including the notice requirement:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication . . . , that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a *warrant issued using the procedures described in the Federal Rules of Criminal Procedure* by a court with jurisdiction over the offense under investigation.

18 U.S.C. § 2703(a) (emphasis added). Contrary to the government’s interpretation of

the statute, it does not contain the word “obtain”. Rather, by its plain terms, the statute describes the manner by which the government may “require” “disclosure.” Nothing in the statute purports to limit its protections to either third party communication holders or the aggrieved subscribers solely to the manner in which a warrant was “obtained.”

The statutory limitation is on “disclosure” “pursuant” “to a warrant issued using procedures described “in the Federal Rules . . .” There is simply nothing in the statutory language to support the government’s contention that the reference to the Federal Rules of Criminal Procedure refers only to those procedures involved in obtaining a warrant.

The error in the government’s reading of the statute is manifest upon reading of subsection (e) of Rule 41, captioned “Issuing the Warrant.” “Issuing” is not limited to obtaining a warrant, as the government contends, but includes the execution and return of the warrant. Rule 41(e) begins in subsection (1) by limiting the persons to whom a judge may give a warrant. In doing so, it employs the word “issue,” clearly indicating that the word encompasses more than the government suggests.

- (1) In general, the magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it.

Subsection (2), captioned “Contents of the Warrant,” then states that the warrant must explicitly include the manner of execution. When issuing a warrant, the court commands the officer to:

- (i) execute the warrant within a specified time no longer than 10 days;
- (ii) execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time; and

(iii) return the warrant to the magistrate judge designated in the warrant.

Fed. R. Crim. P. 41(e)(2). Subsection 41(e)(2) thereby incorporates the manner of execution set out in subsection 41(f), titled Executing and Returning the Warrant. The government's reading would eliminate protections on execution of warrants under § 2703(a), which is inconsistent with the statutory text.

Because no extraordinary circumstances warrant deviation from the statute's plain meaning, "the sole function of the courts is to enforce it according to its terms." *United State v. Ron Pair Enterprises*, 489 U.S. 235, 241 (1989).

B. The Canons Of Statutory Construction Support The Plain Meaning Requiring Notice To The Subscriber or Customer Of The Execution Of A Warrant.

The statute's plain meaning, that all of Rule 41's procedures – including notice as required in Rule 41(f) – are incorporated into § 2703(a), is reinforced by the traditional rules of statutory interpretation.

1. The context of the statute supports the plain meaning.

The larger statutory context is one in which Congress sought to ensure privacy protections for electronic communications. The more specific statutory context establishes that § 2703(a) provided privacy protections including notice, in contrast to other sections that eschewed notice by their plain terms.

It is a basic canon of statutory construction that "where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello v. United States*, 464 U.S. 16, 23 (1983).

Section 2703(b) contains an explicit exception to the notice requirement:

(b) Contents of wire or electronic communications in a remote computing service. – (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) *without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure* by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity –

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

18 U.S.C. § 2703(b). In contrast, subsection (a) does not. Subsection (a) incorporates all the Rule 41 procedures, including its notice provisions, while subsection (b) also incorporates Rule 41, but provides explicit exceptions to the general notice requirement in Rule 41(f). Applying the principle *expressio unis est exclusio alterius*, which assumes that Congress acts carefully and deliberately in including terms in one part of the statute and omitting them in another, the inclusion of the notice exception in § 2703(b) reinforces the plain meaning of the statute to require notice under § 2703(a). *Barnhart v. Peabody Coal Co.*, 537 U.S. 149, 168 (2003),

2. *The government's reading of the statute would render the search warrant provisions in § 2703(b)*

superfluous.

If there were no notice requirement under § 2703(a), as the government contends, then there would be no need for an exception to notice in the search warrant subsection of § 2703(b). It is “a cardinal principle of statutory construction” that “a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.” *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001)(quoting *Duncan v. Walker*, 533 U.S. 167, 174 (2001); *United States v. Menasche*, 348 U.S. 528, 538-539 (1955) (“It is our duty ‘to give effect, if possible, to every clause and word of a statute.’ ” (quoting *Montclair v. Ramsdell*, 107 U.S. 147, 152 (1883))). This is especially true where Congress provides an exception to a general rule – here, that notice is required. *TRW*, 534 U.S. at 28 (“Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent.”).

The government’s reading of the statute would make the exceptions to notice in subsection (b) unnecessary. Section 2703(b) uses the same phrase at issue in this case: “issued using the procedures described in the Federal Rules of Criminal Procedure.” If the government is correct that this language does not incorporate the notice provisions in Rule 41, then the statutory exception to notice – “without required notice to the subscriber or customer” – would have no significance.

Similarly, the government’s reading would render Rule 41(e)’s commands regarding the execution of the warrant irrelevant in this context. Once the government accepts that Rule 41(e) applies, it cannot read the statute to render one of its key

provisions meaningless.

3. *When read in then context of other statutes, § 2703(a) clearly requires notice to the subscriber.*

Subsection 2703 must be interpreted in relation to the whole statutory text. *Dolan v. Postal Service*, 546 U.S. 481, 486 (2006) ("Interpretation of a word or phrase depends upon reading the whole statutory text, considering the purpose and context of the statute, and consulting any precedents or authorities that inform the analysis."). Here, the government's reading of the statute conflicts with other provisions of the SCA incorporating a notice requirement.

Review of § 2704, regarding backup preservation of electronic communications, is particularly instructive. Congress included an express notice requirement to the subscriber or customer if the provider is directed to create a backup copy of the contents:

Notice to the subscriber or customer *shall* be made by the governmental entity, within three days after receipt of such confirmation [that a backup copy has been created], unless such notice is delayed pursuant to section 2705(a).

18 U.S.C. § 2704(a)(2) (emphasis added). There is also a companion notice exception for electronic communications covered by § 2703(b):

A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications. . . . *Without notifying the subscriber or customer of such subpoena or court order*, such service provider shall create such backup copy

18 U.S.C. § 2704(a)(1) (emphasis added). As with § 2703, Congress created a general rule requiring notice and an exception to the notice requirement for documents covered

under § 2703(b). Because the statutes deal with the same subject, they should be read *in pari materia* and harmonized, if possible, especially where, as here, they were enacted at the same time. *Erlenbaugh v. United States*, 409 U.S. 239, 243 (1972).

Moreover, it would be illogical to require notice by the government when it requests that a backup copy be prepared, but no notice when the contents are originally obtained. *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982) ("It is true that interpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available.").

4. *Section 2703 must be interpreted in relation to the overall purpose of the chapter of protecting the subscriber's privacy interests balanced by legitimate law enforcement interests.*

"Interpretation of a word or phrase depends upon reading the whole statutory text, considering the purpose and context of the statute, and consulting any precedents or authorities that inform the analysis." *Dolan*, 546 U.S. at 486. In this case, the purpose of the statute is "to protect the privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." S.Rep. 99-541, 3 *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (1986). Accordingly, the SCA provides in various provisions a general rule against non-disclosure of the contents of electronic communications, followed by exceptions to the general rule. For example, § 2702 prohibits disclosure in subsection (a), and in subsection (b), allows for disclosure to specified persons – generally the recipient or subscriber. Section 2703 follows this format by establishing a general rule in subsection (a) that the government may only obtain the contents of electronic communications, pursuant to Rule 41, followed in subsection (b) with procedures to obtain the information without the notice

requirement.

The requirement for Rule 41 notice procedures must be interpreted in the light of the important policies underlying the § 2703 (a) warrant requirement. It is not just to assure that the government has a legitimate interest in the contents of the electronic communications, but it also serves to “assure[] the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search,” *United States v. Chadwick*, 433 U.S., 1, 9 (1977)²; as well as to “give notice to the person subject to the search what the officers are entitled to seize.” *In the Matter of Seizure of Property Belonging to Talk of the Town Bookstore, Inc.*, 644 F.2d 1317, 1318 (9th Cir.1981). And, as the government acknowledges, a warrant serves as judicial oversight to ensure that the government has not overstepped its legitimate law enforcement interest. The government's reading of § 2703(a) ignores these essential functions. Thus, the purpose and structure of the SCA evidences a clear preference for the privacy of the subscriber, with disclosure only allowed with a warrant and notice.

5. *The legislative history clearly demonstrates that notice to the subscriber is required, unless the court approves of delayed notice.*

If there were any ambiguity about the notice requirement, the legislative history makes it clear that Congress intended that all of the protections afforded through the warrant process were to be available to protect the subscriber's privacy interests.

United States v. Williams, 128 S.Ct. 1830, 1847 (2008) (Stevens, J., concurring, joined by Breyer, J.) (“[T]o the extent the statutory text alone is unclear, our duty to avoid

²Abrogated on other grounds, *California v. Acevedo*, 500 U.S. 565 (1991).

constitutional objections makes it especially appropriate to look beyond the text in order to ascertain the intent of its drafters.”).

Congress enacted § 2703 because information subject to the control of third party computer operators lacked clear constitutional protections and was vulnerable to “unauthorized use and public disclosure by law enforcement officers.” S.Rep. 99-541, 3 *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (1986). The intent of the drafters was to bring electronic communications within the protections of the Fourth Amendment. *Id.* 3556. The Senate explained:

A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. . . . But there are no comparable Federal statutory standards to protect the privacy and security of [electronic communications]. ... This gap results in legal uncertainty. . . . Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

1986 U.S.C.C.A.N. at 3560. Accordingly, Congress clarified that Fourth Amendment protections were extended to electronic communications through the SCA.

As relevant here, Congress required that government entities could only require disclosure of the contents of electronic communications in storage for less than 180 days pursuant to a warrant:

Subsection (a) of section 2703 provides requirements for the government to obtain the contents of an electronic communication that has been in storage for 180 days or less. A government entity can only gain access to the contents of such an electronic communication pursuant to a warrant issued under the Federal Rules of Criminal Procedure or an equivalent State warrant.

1986 U.S.C.C.A.N. at 3592. Congress's intention that the warrant procedure include a notice requirement is also evidenced by the history of § 2705, allowing for delayed notice if necessary:

This proposed section provides procedures and requirements for implementation for a delay of notice to the customer or subscriber that his records are being sought or have been provided to a government entity. Subsection (a) of this section 2705 provides that when a Government entity seeks or obtains access to the contents of an electronic communication by application for a court order, notification can be delayed for an initial period of up to 90 days, if the Government entity requests such a delay and the court determines that there is reason to believe that the notification of the existence of the court order may have an adverse result as described in this subsection.

1986 U.S.C.C.A.N. at 3595. There is nothing in the legislative history to support the government's reading of the statute.

III. The Amendments Promulgated Pursuant To The Patriot Act Did Not Change The Plain and Unambiguous Meaning Of the Statute.

The government is correct that, when Congress alters the words of a statute, it does so with an intent to change the statute's meaning. Gov. Br. at 6 (citing *United States v. Wilson*, 503 U.S. 329, 336 (1992)). However, the 2001 amendments were not intended to, and did not, change the notice requirement. To the contrary, the 2001 amendments were purely jurisdictional and preserve the procedures of Rule 41.

In issuing warrants under § 2703(a) prior to 2001, courts were restricted by the jurisdictional reach of Rule 41(b) to the district where the warrant application was made. This was so because § 2703(a) required that warrants be issued *under* Rule 41, and by its plain terms, Section 2703(a) did not grant any independent authority to issue warrants to judges outside the district where property was located.

Following September 11, 2001, Congress deemed it necessary to expand the

authority to issue warrants for property outside the investigating district. Accordingly, in the Patriot Act, Congress authorized the court with jurisdiction over an investigation to issue a warrant directly. H.R. Rep. 107-236(I), 107th Cong. 1st Sess. 2001). Rule 41(b) is the only subsection implicated in the 2001 amendment to § 2703. That the Patriot Act only addressed Rule 41(b) is evidenced by Senator Leahy's explanation of the jurisdictional nature of the amendments:

This will allow the judge who is most familiar with the developments in a fact-breaking and complex terrorism investigation to make determinations of probable cause, no matter where the property to search is located. This will not only save time by avoiding having to bring up-to-speed another judge in another jurisdiction where the property is located, but also serves privacy and Fourth Amendment interests in ensuring that the most knowledgeable judge makes the determination of probable cause.

147 Cong. Rec. s. 10990, 107th Cong., 1st Sess. (Oct. 25, 2001). There is simply nothing in the Patriot Act amendments to suggest that Congress intended to dispense with notice and limit application of any of the Rule 41 procedures.

The cases upon which the government relies support the jurisdictional nature of the changes and do not stand for the proposition asserted by the government. In *United States v. Berkos*, 543 F.3d 392, 397-98 (7th Cir. 2008), the court discussed the interplay of Rule 41(b) and § 2703(a), and concluded that § 2703(a) authorized out-of-district warrants, but clarified that the procedural provisions of Rule 41 remained intact. The question presented in *In the Matter of the Search of Yahoo* was whether the district court could properly issue a warrant directed to an out-of-district service provider. 2007 WL 1539971 *5 (D.Ariz. 2007). The court concluded that reference to the Federal Rules of Procedure referred not to Rule 41(b) jurisdictional limitations, but to the procedural portions of the Rule. *Id.* See also *In re Search Warrant*, 2005 WL 3844032

(M.D.Fla. 2005) (§ 2703(a) authorizes issuance of out-of-district warrant).

Even if the procedures of Fed. R. Crim. P. incorporated in § 2703 were only those directed to the issuance of warrants, the government's argument fails. Rule 41(e) pertaining to the issuance of warrants provides a mandate for how and when a warrant must be executed and returned. The warrant authority described in Rule 41(e) is a unitary inseverable procedure – what is authorized is the overall warrant procedure rooted in the Fourth Amendment.

To extend the government's faulty logic – that the procedures are limited to obtaining and issuing warrants – would leave open the question of whether there are any rules or procedures for the execution of warrants issued under § 2703(a). As discussed above, the purpose and intent of § 2703(a) are to protect the subscriber's privacy and Fourth Amendment interests. Those interests would hardly be served if the protections were limited to obtaining warrants and not their execution.

IV. If There Were Any Ambiguity, The Doctrine Of Constitutional Avoidance Requires Notice.

To the extent that there is any ambiguity in the statute directing that the procedures for executing warrants must be followed, courts are "obligated to construe the statute to avoid constitutional problems if it is fairly possible to do so." *Boumediene v. Bush*, 128 S.Ct. 2229, 2271 (2008)(citations omitted). "The canon of constitutional avoidance comes into play only when, after the application of ordinary textual analysis, the statute is found to be susceptible of more than one construction; and the canon functions as a means of choosing between them." *Clark v. Martinez*, 543 U.S. 371, 385 (2005). The serious constitutional issues that would arise if the government is

permitted to proceed with no notice are set out below.

A. A Search Pursuant To A Warrant Without Any Notice To The Subscriber Violates The Fourth Amendment.

Eliminating the requirement of any notice is contrary to the Fourth Amendment, the Stored Communications Act (specifically 18 U.S.C. §§ 2703 and 2705), and Federal Rule of Criminal Procedure 41.

1. *E-mails are entitled to the protection of the Constitution and statutes.*

The Fourth Amendment of the United States Constitution provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

While the Supreme Court has not yet addressed the question of the existence of Fourth Amendment privacy interests in e-mail, there should be no question but that such communications are as worthy of the protections of the Fourth Amendment as telephone conversations. Congress recognized and reinforced the reasonableness of an expectation of privacy in e-mails, in the Stored Communications and Electronic Privacy Acts. It did so again in 2002 when Fed. R. Crim. P. 41 was amended to include "information" in the definition of property. See Fed. R. Crim. P. 41(a)(2)(A). Indeed, long before the amendment to the rule, the Supreme Court had stated:

Although Rule 41(h) [now Rule 41(a)(2)(A)] defines property 'to include documents, books, papers, and any other tangible objects,' it does not restrict or purport to exhaustively enumerate all the items which may be seized pursuant to Rule 41. Indeed, we recognized in *Katz v. U.S.*, which held that telephone conversations were protected by the Fourth Amendment, that Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a

finding of probable cause.”
United States v. New York Telephone Co., 434 U.S. 159, 169 (1977).

The fact that Fourth Amendment protections are accorded to telephone conversations was first recognized in *Katz v. United States*, 389 U.S. 347 (1967). See *Smith v. Maryland*, 442 U.S. 735, 740 (1979). The Supreme Court has specifically held that the fact that telephone communications are exposed to third party service providers does not undermine the protected privacy interests. The caller “is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,” and, therefore, has not given up his privacy right in the conversation. *Katz*, 389 U.S. at 352.

While the Supreme Court has not specifically addressed e-mails, the fact that they are entitled to the same protections as afforded to telephone conversations was recognized by the Sixth Circuit in *Warshak v. United States*, 490 F.3d 455, 470 (6th Cir. 2007) (opinion vacated on ripeness grounds). *Warshak* recognized that, under *Katz*, “the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eavesdropping would never amount to a search.” *Warshak*, 490 F.3d at 470. However, the court acknowledged that if you share “communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person.” *Warshak*, 490 F.3d at 470 (citing *United States v. Miller*, 425 U.S. 435, 443 (1976)). The Sixth Circuit then found that:

The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would

never be protected, by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them.

Warshak, 490 F.3d at 470.

Recently, in a case involving the SCA, the Ninth Circuit found that people have a reasonable expectation of privacy in text messages stored on a service provider's network. *Quon v. Arch Wireless Operating Company, Inc.*, 529 F.3d 892, 904 (9th Cir. 2008). *See also United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) ("The contents [of e-mails] may deserve Fourth Amendment protection.").

While the Ninth Circuit has not specifically addressed the protections to be afforded e-mails, it has recognized that the fact that a computer is connected to a network does not undermine the rights of privacy held by its owner. In *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007), the court found that a university student had a reasonable expectation of privacy in his computer files even though he "attached [his computer] to the university network," because the "university policies [did] not eliminate [his] expectation of privacy in his computer." Even though the policies included situations in which the university administrators could access his computer, this was not a blanket monitoring or auditing policy so it was insufficient to waive the user's expectation of privacy. *Id.*; *see United States v. Barth*, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (holding that defendant retains a reasonable expectation of privacy in computer files contained in hard drive left with computer technician for limited purpose of repairing computer); *see also Ex parte Jackson*, 96 U.S. 727, 733 (1878) ("No law of Congress can place in the hands of officials connected with the

postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.”).³

2. *Notice to the Subscriber Is Required in Order to Comply with the Fourth Amendment and Fed. R. Crim. P. 41 When A Search Is Conducted For The Content Of E-mails.*

The Stored Communications Act provides subscribers with many privacy protections consistent with the Fourth Amendment. As explained above, the Act did not eliminate the notice requirement provided in Rule 41 and the Fourth Amendment. Nor could it without running afoul of the constitution.

In those cases, the government seeks to conceal from the subscribers that a search ever took place. What prompts this motivation is unknown. Regardless of this motivation, the Fourth Amendment does not allow the government to execute a lawfully obtained search warrant and then conceal it from those the Amendment protects.⁴ In

³At issue here are the contents of communications, not mere subscriber information or other less intrusive information that can be obtained from, for example, a pen register. See *Smith*, 442 U.S. at 741; *Warshak*, 490 F.3d at 471.

⁴The Courts have held that notice may be delayed in limited circumstances. See *Dalia v. United States*, 441 U.S. 238, 247 (1979). The period of delay must, however, be reasonable. *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986). While not presented in this appeal, it may well be that the bounds of reason were passed in the period of delay that was authorized in this case. See *United States v. Villegas*, 899 F.2d 1324, 1338 (2d Cir. 1990) (“While we do not suggest that extensions could be granted indefinitely, we conclude that the tolerable limit was not exceeded in this case.”). Why the government now seeks to eliminate any notice requirement, versus simply extending the delay in notice until an appropriate time, is unexplained. In response to the government’s attempts to eliminate the notice requirement, this brief only addresses the distinction between notice, even when delayed, and *no* notice of the search.

Berger, the Supreme Court struck down a state wiretapping statute because it had “no requirement for notice as do conventional warrants, nor [did] it overcome this defect by requires some showing of special facts. On the contrary, it permit[ed] uncontested entry without any showing of exigent circumstances.” 388 U.S. 41 at 60. In the case of conventional search warrants that are executed when the occupants are absent, Rule 41 requires that notice be left that a search took place.

The notice requirement in Fed. R. Crim. P. 41(f) is grounded in the Fourth Amendment. See *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986) (*Freitas I*) (finding that warrant for surreptitious entry into a home violated the Fourth Amendment by failing to provide notice as required by former Rule 41(d)). In *Freitas I*, the Ninth Circuit stated:

The absence of a notice requirement in the warrant presents a much more difficult issue. While it is clear that the Fourth Amendment does not prohibit all surreptitious entries, see *Dalia v. United States*, 441 U.S. 238, 247 . . . (1979), it is also clear that the absence of any notice requirement in the warrant casts strong doubt on its constitutional adequacy, see *Berger v. New York*, 388 U.S. 41, 60 . . . (1967). We resolve those doubts by holding that in this case the warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed seven days except upon a strong showing of necessity.

We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed. The warrant in this case failed to do so.

Freitas, 800 F.2d at 1456. *Freitas* relied on the statements in *Dalia v. United States*, 441 U.S. 238 (1979), regarding the need for notice in telephone monitoring under a

Title VII warrant. 800 F.2d at 1456 (citing *Dalia*, 441 U.S. at 247). *Freitas I* was reaffirmed in *Freitas II*, *United States v. Freitas*, 856 F.2d 1425 (9th Cir. 1988). A decade later, the Ninth Circuit again addressed the need for notice in *Gantt*, in the context of a search for physical evidence. 194 F.3d at 1001. There the court upheld the seizure based on a “constitutionally adequate substitute” for advance notice in the requirements in Title III for notice once the surveillance was completed.

The Fourth Amendment provides protection for a *person’s* privacy, not simply places. “[O]nce it is recognized that the Fourth Amendment protects people - - and not simply ‘areas’ - - against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.” *Katz*, 389 U.S. at 353. When a subscriber’s e-mails are searched by the government, that subscriber is an aggrieved person. That aggrieved person must receive notice of that search in order for the search to be considered reasonable. *Gerstein v. Pugh*, 420 U.S. 103, 116 n. 17 (1975).

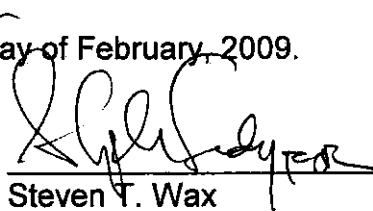
The government suggests that if notice is required, notice to the third party intermediary is sufficient. However, this cannot be the case. The third party intermediary has a far lesser privacy interest in the content of its subscribers’s e-mails than the subscribers themselves. As Judge Hubel stated, “[t]o have any meaning, . . . the required notice is to the subscriber to the e-mail service. Indeed, with the order to the service provider not to disclose the issuance of the warrant and its execution to anyone, notice to the service provider accomplishes nothing.” Order at 7.

Conclusion

When Magistrate Judge Hubel was presented with the application for search

warrant in this case, it was with the approval for delayed notice that e-mails were searched, not as notice. Basic principles of statutory construction reveal that 18 U.S.C. § 2703(a) requires notice that is sufficient pursuant to the Fourth Amendment and Fed. R. Crim. P. 41(f). The doctrine of constitutional avoidance supports this reading because the Constitution requires notice. The government cannot now conceal the fact that a search took place from the subscriber without violating the statute or Constitution. This Court should affirm Judge Hubel's order.

Respectfully submitted this 20th day of February, 2009.

A handwritten signature in black ink, appearing to read "Steven T. Wax", is written over a horizontal line.

Steven T. Wax
Amicus Curiae

Lynn Deffebach and Michelle Sweet
Assisting on the Brief

CERTIFICATE OF SERVICE

I hereby certify that I made service of the foregoing **BRIEF OF AMICUS CURIAE FILED UNDER SEAL** on Assistant U.S. Attorney Hannah Horsley by hand delivering on February 20, 2009, a true, exact, and full copy thereof, addressed to 600 U.S. Courthouse, 1000 SW Third Avenue, Portland, Oregon 97204.


Sandra L. Showard

CERTIFICATE OF SERVICE